## REMARKS

Applicant respectfully traverses and requests reconsideration.

Claims 1, 15, 18, 20 and 24 stand objected to due to typographical errors. Applicant has amended the claims as suggested by the Examiner. As such, Applicant respectfully requests that the objection be withdrawn. As to claim 15, Applicant has also corrected the typographical error and as such, Applicant respectfully requests that the objection be withdrawn.

Claims 1-8, 10, 12, 15-24 and 28 stand rejected under 35 U.S.C. §102(e) as being anticipated by Perlman et al. As to the independent claims, they require, among other things for example, receiving encrypted information from a sender for transmission to at least one intended recipient and receiving an encrypted secret key encrypted using a public key associated with a secure distribution server. The office action cites the "DLE 110 and group server 114 (column 5, lines 28-31 and column 7, lines 41-59)" (page 4 of rejection) as allegedly teaching this subject matter. However, Applicant respectfully wishes to point out that as claimed, the encrypted secret key is encrypted using a public key associated with a secure distribution server and as such, the secure distribution server has a public key which is used to encrypt a secret key. Accordingly, the secure distribution server as claimed is a trusted entity whose public key is used to encrypt the secret key which is then later decrypted and then re-encrypted and forwarded as claimed.

Perlman teaches a very different approach. In fact, the cited portions state that the key used to encrypt the secret key of Perlman is a "group public key 107" (column 5, line 29). As such, the group public key – not a secure distribution server key – is used to encrypt the secret key. The "group public key 107" of Perlman is independent of the DLE 110 and group server 114. As such, the cited reference does not teach the claimed subject matter and the claim is in condition for allowance. Also, Applicant respectfully notes that the cited portion of column 7

actually refers to an option "B" which occurs after the message key has been encrypted as shown, for example, in FIG. 4a. The encrypted message key is encrypted using the "group public key" as taught by Perlman. This "group public key" is independent of the DLE or group server 114. In fact, a different group recipient key is generated for different groups. In contrast, Applicant claims an encrypted secret key that is encrypted using a public key associated with a secure distribution server. As such, Applicant claims encrypting the secret key using a public key that is independent of a group of recipients or recipient and instead is the public key associated with the secure distribution server. For example, see Specification paragraph 22 and elsewhere noting that the public key associated with the secure distribution server (PkSDS) is used to encrypt the secret key. No such DLE key or group server key is described or utilized to encrypt the secret key of Perlman as claimed. Accordingly, Applicant respectfully submits that the independent claims are in condition for allowance.

The dependent claims add additional novel and non-obvious subject matter. For example, claim 4 requires that the secret key is encrypted with the public key associated with the secure distribution server to produce the encrypted secret key and sending the encrypted information and the encrypted secret key to the secure distribution server. As such, the secure distribution server receives an encrypted secret key and encrypted information wherein the encrypted secret key that it receives is encrypted with a public key of the secure distribution server so that the secure distribution server can use its private key to decrypt the secret key. The secure distribution server is a trusted entity since the sender uses the public key of the secure distribution server to encrypt the secret key. Such operation as noted above is not taught in the cited portions of Perlman.

In addition, claim 5 requires that the secret key is encrypted using a public key for each of a plurality of secure distribution servers to produce a plurality of secure distribution server specific encrypted secret keys. The office action cites FIG. 4a-4c and column 4, lines 47-51 as allegedly teaching this subject matter. However, the cited portion merely states that a plurality of servers are involved in the process of encrypting and forwarding email messages. As set forth throughout the specification of Perlman which actually describes the actual implementation of Perlman, and as noted above, there is no secure distribution server public key that is used to encrypt the secret key in the cited portions. In fact, as mentioned above with respect to FIG. 4a, it is only a group recipient key that is used in the initial encryption of the secret key process in Perlman. Such a key is independent of the DLE and group server 114 alleged to equate with the claimed secure distribution server. Accordingly, Applicant respectfully submits that there are no public keys for each of the secure distribution servers in Perlman and as such, this claim is also in condition for allowance.

The other dependent claims add additional novel and non-obvious subject matter.

Claims 9, 13 and 25 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Perlman. Applicant respectfully submits that the mere forwarding and routing packets by nodes in the network is not equivalent to what is being claimed. Applicant respectfully notes that the claims cannot be parsed in such a manner as to ignore specific claim language. For example, in the context of claim 9 which depends on claim 1, not only is encrypted information received from a sender the encrypted key using a public key of the secure distribution server is also received. Also, the claim includes receiving the encrypted information and the encrypted secret key and forwarding the same to the secure distribution server without decrypting the encrypted secret key. Since the rejection of claim 1 attempts to equate the DLE and group server 114 of

Perlman with the claimed secure distribution server, claim 9 requires that the encrypted information is also forwarded to the secure distribution server. However, the teachings of Perlman would not allow the forwarding and routing of packets in the nodes in a network to take effect as alleged in the office action since Perlman in fact teaches not to send the encrypted message to the group server. For example, as shown in FIG. 3, all that the group server receives is the encrypted message key. The recipient performs the decryption and receives the encrypted message. As such, blindly including the forwarding and routing of packets as alleged in the office action to that of Perlman would materially change the operation of Perlman which as admitted in Perlman "can greatly compromise the system security" (see column 6, lines 1-8). Applicant respectfully submits that the combination as alleged is incompatible with the teachings of Perlman and as such, the claims are in condition for allowance.

Claims 11 and 27 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Perlman in view of Chen. Applicant respectfully reasserts the relevant remarks made above with respect to Perlman and as such, these claims are also in condition for allowance.

Claim 14 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Perlman in view of Bouchard et al. Applicant respectfully reasserts the relevant remarks made above with respect to Perlman and as such, this claim is also in condition for allowance. The claim also adds additional novel and non-obvious subject matter.

Applicant respectfully requests that a timely Notice of Allowance be issued in this case. The Examiner is invited to contact the below-listed attorney if the Examiner believes that a telephone conference will advance the prosecution of this application.

Respectfully submitted,

Date: 7-11-07

By: _____
Christopher J. Reckamp
Registration No. 34,414

Vedder, Price, Kaufman & Kammholz, P.C.
222 N. LaSalle Street
Chicago, Illinois 60601
PHONE: (312) 609-7599
FAX: (312) 609-5005